## REMARKS/ARGUMENTS

Favorable reconsideration and allowance of the present application are respectfully requested in view of the following remarks. Claims 1-25 remain, of which claims 1, 15 and 24 are independent.

Claims 1, 4-5 and 7 are amended only to address informal and procedural issues. The scope of the claims remain unchanged. Applicant respectfully request that the amendments be entered.

In the Office Action, the Examiner makes the following rejections:

- claims 1-5, 7-13, 15-22, 24 and 25 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Haverinen et al. (U.S. Publication No. 2002/0012433) in view of Ala-Laurila et al. (U.S. Publication No. 2002/0009199);
- claim 6 stands rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Haverinen et al. in view of Fink et al. (U.S. Patent No. 7,043,633); and
- claims 14 and 23 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Haverinen et al. in view of Amin et al. (U.S. Patent No. 6,854,014).

Applicants respectfully traverse all prior art based rejections. The present application claims a method in a telecommunication system for allowing a SIM-based authentication to users of a wireless local area network who are subscribers of a public land mobile network. The method includes a

step of carrying out a challenge-response authentication procedure between a wireless terminal and a public land mobile through an Access Controller, which is interposed between an Access point and the PLMN. The wireless terminal is provided with a SIM card and adapted for reading data thereof.

The challenge-response authentication submissions takes place before having provided IP connectivity to the user, i.e., before having been provided to the wireless terminal. Between the wireless terminal and the Access controller, the challenge-response submissions are carried on top of a Point-to-Point layer 2 protocol (PPPoE). Between the Access Controller and the PLMN, the challenge-response submissions are carried on an authentication protocol residing at an application layer. That is, the authentication between the wireless terminal and the public land mobile network is carried out on top of a Point-to-Point layer 2 protocol between the wireless terminal and the Access Controller and on an authentication protocol residing at application layer between the Access Controller and the public land mobile network.

Once the subscriber has been authenticated, an IP address is allocated to the wireless terminal and the subscriber is given IP connectivity. In other words, the authentication of the subscriber to the PLMN is not carried out over IP in the present application, and does not require allocating an IP address to the wireless terminal for carrying out the SIM-based authentication procedure.

The Examiner admits that Haverinen et al does not teach or suggest the feature of allocating an IP address after having authenticated the subscriber,

but alleges that paragraph [0020] of Ala-Laurila et al. discloses the feature. Paragraph [0020] states, "In accordance with a preferred embodiment it allocates an IP address to the terminal MT and allows a connection to be established to the internet only if the terminal MT can be authenticated". From this statement alone, Examiner alleges that the feature of allocating the IP address only after terminal MT is authenticated. Even when taken out of context, this statement at best indicates that the connection to the internet is allowed when the MT is authenticated. The statement does not rule out allocating the IP address prior to the authentication for use in communication between the MT, PAC, and the public land mobile network (PLMN) during the authentication process.

Indeed, the MT of Ala-Laurila et al. cannot be authenticated by the public land mobile network unless the MT is assigned an IP address prior to authentication, as well as IP addresses being also respectively assigned to PAC and GAGW, as disclosed on paragraph [0023]. In this respect, the GSMNW (example PLMN) illustrated in Fig. 1 of Ala-Laurila et al. communicates with the PAC and the MT through an IP network; paragraphs [0021]-[0022] describe the entities involved in both WLAN network and GSMNW on authenticating the subscriber.

In paragraph [0023], Ala-Laurila et al. specifically states, "The interfaces between the terminal MT and the controller PAC and between the PAC and the GAGW <u>are IP-based</u> in accordance with a preferred embodiment." *Emphasis*

*added.* Ala-Laurila et al. further discloses in paragraph [0023] "... MT, PAC and GAGW are identified using IP addresses" which further indicates that an IP network is used between the MT, WLAN and the GSMNW.

No other enabling embodiment is disclosed in Ala-Laurila et al. showing how MT, PAC and GAGW can carry out the authentication procedure and, even less, to what end the intermediate IP network is then used. Moreover, there is no disclosure in Ala-Laurila et al. of further handling of security keys having alternative intermediate networks, a non-IP network for communicating the WLAN network with the GSMNW for authentication purposes and an IP network for other purposes.

In paragraph [0024], Ala-Laurila et al. states "Before the terminal MT is allowed to establish a connection with other networks than the network WLAN, the authentication must be performed in an acceptable manner." *Emphasis added.* This indicates that MT communicates with GAGW during authentication with PAC therebetween. Ala-Laurila indicates that all communication between MT, PAC and GAGW are conducted using IP. Thus, the only conclusion that can be reached is that the authentication procedure carried out between the MT, PAC and the GAGW requires a previous allocation of IP addresses to all these three entities.

As shown, under Ala-Laurila, MT is provided with IP connectivity prior to authentication. The IP connectivity may be internally limited by the WLAN network until successfully completing the authentication procedure. But this

does not negate that fact that IP connectivity is still provided before authentication. Therefore, Ala-Laurila et al. fails to disclose a SIM-based authentication of the subscriber successfully performed before allocating an IP address and offering IP connectivity to the wireless terminal.

Examiner may be interpreting paragraph [0020] to mean Ala-Laurila et al. discloses authenticating the MT by the WLAN network and, after having been successfully authenticated by the WLAN network, an IP address is allocated to the MT and PAC for carrying out the SIM-based authentication with the GSMNW. Known procedures such as WEP and WPA are examples of such authentication procedures. *See Fig. 3; paragraphs [0045]-[0046].* These procedures only involve the MT and the WLAN. In contrast, the challenge-response authentication procedure is carried out between the wireless terminal and the public land mobile network through the Access Controller in claim 1.

In Ala-Laurila et al., once the WLAN authentication has been successfully carried out, the authenticated wireless terminal (MT) is allocated the IP address as referred to in paragraph [0024]. Furthermore, once the MT has been authenticated by the WLAN network and has been allocated the IP address to access the public land network GSMNW, the SIM-based authentication with the GSMNW explained in paragraphs [0021]-[0023] and illustrated in Fig. 2 is carried out as Ala-Laurila et al. discloses on paragraph [0047]. That is Ala-Laurila et al. discloses an authentication of the MT by the WLAN network (an exemplary WEP procedure), followed by the allocation of an

IP address and IP connectivity to access the public network GSMNW, and a further SIM-based authentication of the MT by the GSMNW.

Consequently, Ala-Laurila et al. fails to disclose a SIM-based authentication of the subscriber successfully performed before allocating an IP address and offering IP connectivity to the wireless terminal, as claimed in claim 1 of the present application. None of Haverinen et al., Fink et al., and Amin et al. disclose corrects the above noted deficiencies of Ala-Laurila. Therefore, independent claim 1 is distinguishable over all any combination of the applied references. For similar reasons, independent claims 15 and 24 are also distinguishable over the same references. By virtue of their dependencies from independent claims as well as on their own, dependent claims 2-14, 16-23 and 25 are distinguishable over any combination of the same references.

Applicants respectfully request that the rejections of claims 1-25 be withdrawn.

All objections and rejections raised in the Office Action having been addressed, it is respectfully submitted that the present application is in condition for allowance. Should there be any outstanding matters that need to be resolved, the Examiner is respectfully requested to contact Hyung Sohn (Reg. No. 44,346), to conduct an interview in an effort to expedite prosecution in connection with the present application.

The Commissioner is authorized to charge the undersigned's deposit account #14-1140 in whatever amount is necessary for entry of these papers and the continued pendency of the captioned application.

Respectfully submitted,

**NIXON & VANDERHYE P.C.**

By: _____
Hyung N. Sohn
Reg. No. 44,346

HNS/edg
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100